UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA

STEPHANIE MONTGOMERY, *on behalf of herself and all others similarly situated*, Plaintiff, v. 1ST SOURCE BANK, Defendant.	**CASE NO. 3:23-cv-00715-DRL-MGG** **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Stephanie Montgomery ("Plaintiff") brings this Class Action Complaint against 1st Source Bank ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including, but not limited to, Plaintiff's and roughly 450,000 Class Members' names, Social Security numbers, driver's license or state identification card numbers, other government-issued identification numbers, and/or dates of birth (collectively, "Private Information" or "PII").

2. Defendant is a commercial and consumer bank located in South Bend, Indiana and is a wholly owned subsidiary of 1st Source Corporation. Defendant services customers in the northern-Indiana and southwestern-Michigan area.

3. Defendant states that it is the "largest locally controlled financial institution headquartered in the northern Indiana-southwestern Michigan are with nearly $8 billion in assets and more than 1100 employees."[1]

4. Defendant collected, stored, and utilized Plaintiff's and Class Members' Private Information in the regular course of its business for hiring and employment purposes. By obtaining, collecting, using, and deriving a benefit from the Private Information, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. By voluntarily undertaking the collection of this sensitive Private Information, Defendant assumed a duty to use due care to protect that information.

5. Plaintiff provided her Private Information to Defendant as a requisite to receive banking services from Defendant.

6. Despite its duties to Plaintiff and Class Members, Defendant stored their Private Information on a database that was negligently and/or recklessly configured. This misconfiguration allowed files on the database to be accessed without a password or any form of multifactor authentication.

7. On or about June 1, 2023, Defendant was informed of vulnerability in the MOVEit file transfer program Defendant used to transfer to its customers' PII,[2] and that Plaintiff and roughly 450,000 Class Members' Private Information may have been acquired by an unauthorized cybercriminal organization known as the Clop ransomware gang (the "Data Breach").

8. Defendant did not send notice to Plaintiff and Class Members until July 14, 2023 ("Notice of Data Breach").

---

[1] *About Us*, 1st Source Bank, https://www.1stsource.com/about/ (last visited July 27, 2023).

[2] Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/ecd3f2c2-8cdf-48cc-84f5-f3321ae41cd7.shtml (las visited July 27, 2023).

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that it collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been stolen by criminals and listed for sale on the dark web.

10. Upon information and belief, Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on a database that was not password protected and therefore accessible to any member of the public. Foreseeably, cybercriminals exploited this obvious vulnerability, exfiltrated Plaintiff's and Class Members' Private Information from the database, and then listed this information for sale on the dark web.

11. As a result of the Data Breach, Plaintiff and roughly 450,000 Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, the diminished value of their Private Information, and the substantial and imminent risk of identity theft. Given the theft of information that is largely static—like Social Security numbers—this risk will remain with Plaintiff and Class Members for the rest of their lives.

12. As a result of Defendant's failures and the Data Breach, Plaintiff and Class Members' identities are now at a current, imminent, and ongoing risk of identity theft.

13. The risk of identity theft is not speculative or hypothetical but is impending as there is evidence that Plaintiff and Class members' Private Information was targeted, accessed, and possibly disseminated on the Dark Web.

14. Upon information and belief, Plaintiff's and Class Members' Private Information remains in Defendant's possession. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe and should be provided injunctive and other equitable relief.

15. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed in the Data Breach and seeks remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

PARTIES

16. Plaintiff Stephanie Montgomery is a citizen of Indiana residing in South Bend, Indiana.

17. Defendant 1st Source Bank is a domestic for-profit corporation organized under the laws of Indiana with its headquarters and principal place of business located at 100 N. Michigan St., South Bend, Indiana 46601.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members exceeds 100, many of whom have different citizenship from Defendant, including at least 611 Massachusetts residents and 90 Maine residents.[3] Additionally, this action arises out of the same transaction or occurrence as the related

[3] *Data Breach Notifications*, Office of the Maine Attorney General (Defendant's Data Breach Notification to the Maine Attorney General's Office identifying 90 Maine residents affected by the Data Breach), https://apps.web.maine.gov/online/aeviewer/ME/40/ecd3f2c2-8cdf-48cc-84f5-f3321ae41cd7.shtml (last visited Aug. 14, 2023); *Data Breach Notification Report*, Commonwealth of Massachusetts Office of Consumer Affairs and Bus. Regulation (Defendant's

action *Roy Funk v. 1st Source Corporation*, Case No. 3:23-CV-00697 (July 25, 2023), in which Plaintiff Roy Funk is a citizen of Idaho. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

FACTUAL ALLEGATIONS

Background

21. In the ordinary course of its business practices, Defendant acquires, stores, maintains, and uses Plaintiff's and Class Members' Private Information.

22. To obtain banking services, Plaintiff and Class Members provided Defendant, directly or through its associates and franchises, with, among other information, first and last names, home addresses, dates of birth, financial information, photo ID and/or driver's licenses, email addresses, phone numbers, and social security numbers.

23. Defendant agreed to and undertook legal duties to maintain the Private Information of Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should

disclosure of Data Breach to the Massachusetts Office of Consumer affairs identifying 611 Massachusetts residents whose Private Information was affected by the Data Breach, https://www.mass.gov/doc/data-breach-report-2023/download (last visited Aug. 14, 2023).

have known that it was responsible to protect Plaintiff's and Class Members' Private Information from unauthorized disclosure.

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

26. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosure of this Private Information.

27. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, meaning it does not change, and can be used to commit myriad financial crimes.

28. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

29. Defendant had a duty created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

30. In early-to-mid-June 2023, Defendant discovered that an unauthorized party gained access to one of Defendant's vendor's internal file transfer systems resulting in the Data Breach.[4]

[4] *Id.*

31. Upon information and belief, a vulnerability in Defendant's vendor's file transfer system was first discovered in May of 2023.

32. Upon information and belief, Clop was aware of Defendant's vendor's system vulnerability and utilized and exploited before it was discovered by Defendant or its agents, contractors, vendors, and/or suppliers under Defendant's supervision.

33. Defendant failed to adequately monitor its vendor's system and failed to timely detect the Data Breach.

34. On or around July 14, 2023, Defendant notified Plaintiff and Class Members of the Data Breach (the "Notice of Data Breach), stating:

> **What Happened?** On June 1, 2023, we became aware of an alert issued by Progress Software – the company responsible for the MOVEit file transfer program – addressing a critical vulnerability affecting MOVEit, a solution used widely by businesses and government agencies, including 1st Source Bank, to securely transfer data. After becoming aware of the alert, we took immediate steps to patch our MOVEit system in accordance with Progress Software's instructions and conduct an internal assessment. 1st Source thereafter engaged leading, independent cybersecurity experts to conduct a comprehensive investigation to determine the scope of potentially affected data. On June 24, 2023, we learned that your data was contained within a file that may have been acquired without authorization in connection with the MOVEit software vulnerability. Since that time, we have been collecting information needed to provide notice to potentially impacted individuals, including you.
>
> **What Information is Involved?** The information potentially impacted in connection with this incident may have included your name as well as your Social Security number, driver's license or state identification card number, other government-issued identification number, and/or date of birth.

35. Defendant's Notice of Data Breach admits that Plaintiff's and Class Members' Private Information was accessed via an external system data breach without authorization.

36. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's database, and then access and exfiltrate Plaintiff's and Class Members' Private Information stored on Defendant's database. This Private Information was then likely listed for sale on the dark web as that is the *modus operandi* of cybercriminals.

37. Defendant created the risk of the Data Breach by failing to properly configure its database, allowing it to be accessed without a password or any form of multi-factor authentication. Defendant knew or should have known this, and as such owed Plaintiff and Class members a duty of due care to protect their Private Information.

38. Defendant's data security measures were particularly important in light of the substantial increase in cyberattacks on financial institutions in recent years.

39. Because of the sensitive nature of the Private Information that Plaintiff and Class Members provided Defendant, Defendant knew or should have known that its clients' records would be targeted by cybercriminals. However, Defendant failed to monitor its vendors, suppliers, agents, and or contractors in their handling and security of Plaintiff and Class Members' Private Information and failed to maintain reasonable security safeguards and protocols to adequately protect Class Members' Private Information, making them an ideal target for cybercriminals.

Plaintiff Stephanie Montgomery's Experience

40. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

41. Plaintiff only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic security measures to protect her Private Information, such as requiring passwords and multi-factor authentication to access databases storing her Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

42. Plaintiff received a letter from Defendant dated July 14, 2023, informing her of the Data Breach. This letter stated that, among the impacted information, the Data Breach "included [her] name as well as [her] Social Security number, driver's license or state identification card number, other government-issued identification number, and/or date of birth."

43. Plaintiff suffered injury from a loss of privacy the moment that her Private Information was accessed and exfiltrated by a third party without authorization.

44. Plaintiff has also suffered injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her Private Information was placed on a publicly accessible database and exfiltrated by cybercriminals to later be placed on the dark web for sale.

45. The Data Breach has also caused Plaintiff to suffer imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

46. This risk from the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent

activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

47. Defendant acknowledges the risk posed to Plaintiff and her Private Information. Indeed, Defendant has offered a 12-month credit monitoring service via Kroll.

48. The substantial risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

49. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

The Data Breach Was Foreseeable

50. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[5]

51. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the service industry preceding the date of the breach.

52. In 2018, there were 1,257 publicly reported data breaches in the United States and 1,473 in 2019.[6] In 2021, there were 1,862 data breaches in the United States alone.[7]

---

[5] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Mar. 25, 2023).

[6] Abi Tunggal, 116 Must-Know Data Breach Statistics for 2023, UpGuard.com, https://www.upguard.com/blog/data-breach-statistics (last vistied Apr. 20, 2023).

[7] Ani Petrosyan, *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2022*, Statista.com, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/#:~:text=In%202022%2C%20the%20number%20of,have%20one%20thing%20in%20common. (last visited Apr. 20, 2023).

53. In light of the ever-increasing trend of cybersecurity incidents affecting all industries, Defendant knew or should have known that its customers' financial electronic records would be targeted by cybercriminals.

54. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Value of PII

55. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

56. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts.

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Mar. 25, 2023).

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Mar. 25, 2023).

[10] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Mar. 25, 2023).

57. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information…[is] worth more than 10x on the black market."[11]

58. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[12]

59. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

60. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

---

[11] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 25, 2023).

[12] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

62. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

63. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

64. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

65. Plaintiff and the Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant Failed to Properly Protect Plaintiff's and Class Members' Private Information

66. Defendant could have prevented this Data Breach by properly monitoring, securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

67. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

68. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

69. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[13]

70. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

71. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect

[13] *Id.* at 3-4.

cyberattacks. Instead, Defendant failed to implement basic security measures, like password protection, encryption, or multifactor authentication.

Defendant Failed to Comply with FTC Guidelines

72. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

73. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[14]

74. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

75. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[14] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions clarify the measures businesses take to meet their data security obligations.

76. Defendant failed to properly implement basic data security practices, such as making a database storing Private Information available to the public without the use of a password or multifactor authentication.

77. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

78. Defendant was always fully aware of its obligation to protect the PII of Plaintiff and Class members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

79. Several best practices have been identified that at a minimum should be implemented by service providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

80. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

81. The foregoing frameworks are existing and applicable industry standards in the legal industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant Failed to Comply with the Gramm-Leach-Bliley Act

82. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [the Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

83. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Bank Defendants were subject to the requirements of the GLBA, 15 U.S.C. § 6801.1, *et seq.*, and are subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. § 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

84. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

85. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4(a) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and

conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4(a)(1) and 313.5(a)(1); 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9(a); 12 C.F.R. § 1016.9. As alleged herein, Bank Defendants violated the Privacy Rule and Regulation P.

86. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on its network.

87. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

88. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (a) designating one or more employees to coordinate the information security program; (b) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer

information, and assessing the sufficiency of any safeguards in place to control those risks; (c) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (d) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (e) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

89. Defendant failed to assess reasonably foreseeable risks to its networks, and the security, confidentiality, and integrity of PII in its custody or control. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

90. Defendant failed to adequately oversee service providers.

91. Defendant failed to evaluate and adjust their information security programs in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

As a Result of Defendant's Failure to Safeguard Private Information, Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft and Have Experienced Substantial Harm

92. Plaintiff and members of the proposed Class have suffered injury from the access to, and misuse of, their PII that can be directly traced to Defendant.

93. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial

information such as that person's name, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

94. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

95. According to experts, one out of four data breach notification recipients become a victim of identity fraud.

96. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

97. One such example of criminals using PII for profit, to the detriment of Plaintiff and the Class Members, is the development of "Fullz" packages.

98. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

99. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

100. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

101. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen, and in fact did not notify Plaintiff for three months.

102. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

103. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

104. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

105. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[15] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

[15] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited October 10, 2022).

106. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Plaintiff's and Class Members' Damages

107. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services to Plaintiff and Class Members, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

108. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant only offered Class Members credit monitoring, and places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, or time and money signing up for other services, as opposed to automatically enrolling all victims of this Data Breach.

109. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

110. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

111. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

112. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

113. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

114. Plaintiff and Class Members may also incur out-of-pocket costs for further protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

115. Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

116. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security number, bank accounts, and credit reports for unauthorized activity for years to come.

117. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is encrypted and password protected.

CLASS ALLEGATIONS

118. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

119. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around July 14, 2023 (the "Class").

120. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

121. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

122. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are certainly tens of thousands, and possibly in excess of 450,000 individuals whose Private Information was improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

123. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

d. Whether and when Defendant actually learned of the Data Breach;

e. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

f. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

i. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

j. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

124. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

125. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

126. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

127. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action

treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

128. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

129. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

130. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

131. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

132. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

133. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

134. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

135. Plaintiff and the Class entrusted Defendant with their Private Information.

136. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

137. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

138. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

139. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant undertook a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed

to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class Members in Defendant's possession was adequately secured and protected.

140. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information they were no longer required to retain pursuant to regulations.

141. By accepting, storing, and maintaining Plaintiff's and Class Members' Private Information, Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

142. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

143. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

144. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

145. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

146. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

147. Defendant knew or should have known that Plaintiff's and Class Members' Private Information was stored on its database and was or should have been aware of the extreme risks associated with failing to properly safeguard Plaintiff's and Class Members' Private Information.

148. Despite being aware of the likelihood that Defendant's databases were vulnerable, not secure, and likely to be attacked by cybercriminals, Defendant failed to correct, update, or upgrade its security protections, thus causing the Data Breach.

149. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

150. Defendant was in the best position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

151. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Info by third parties.

152. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

153. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C § 45, which prohibits "unfair . . . practice in or affecting commerce," including the unfair practice of failing to use reasonable measures to protect confidential data.

154. Defendant has admitted that the Private Information of Plaintiff and Class Members was improperly accessed and exfiltrated by unauthorized third persons as a result of the Data Breach.

155. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

156. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

157. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

158. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

159. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it wase no longer required to retain pursuant to regulations.

160. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

161. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

162. Said differently, if Defendant had properly supervised its files and vendors' services, then the Data Breach would not have occurred, and Plaintiff's and Class Members' Private Information would have been appropriately safeguarded.

163. Plaintiff and Class Members suffered an injury when their Private Information was accessed by known cybercriminals CLOP.

164. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, and increased risk of imminent harm, suffered by Plaintiff and the Nationwide Class.

165. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

166. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual

and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

167. As a direct and proximate result of Defendant' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

168. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages in an amount to be proven at trial.

169. In addition to monetary relief, Plaintiff and Class Members are entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and supervision procedures, and conduct periodic audits of those systems.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

170. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

171. Plaintiff and Class Members were required to provide Defendant with their Private Information.

172. By Plaintiff and Class Members providing their Private Information, and by Defendant accepting this Private Information, the parties mutually assented to implied contracts. These implied contracts included an implicit agreement and understanding that (1) Defendant would adequately safeguard Plaintiff's and Class Members' Private Information from foreseeable threats, (2) that Defendant would delete the information of Plaintiff and Class Members once it no longer had a legitimate need; and (3) that Defendant would provide Plaintiff and Class Members with notice within a reasonable amount of time after suffering a data breach.

173. Defendant provided consideration by providing banking services in exchange for Plaintiff's and Class Members' PII, while Plaintiff and Class Members provided consideration by providing valuable property, their Private Information. Defendant benefitted from the receipt of this Private Information by being able to utilize Plaintiff and Class Members' employment. In exchange for the Private Information, Defendant promised to protect their PII from unauthorized disclosure.

174. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

175. Defendant materially breached its implied contracts with Plaintiff and Class Members when it (1) allowed third parties to access, copy, and exfiltrate Plaintiff and Class Members' Private Information without permission; and (2) waited an unreasonably long time to notify them of the Data Breach. It is common sense that Plaintiff and Class Members would not have provided Defendant with their Private Information had they known that Defendant would not

implement basic data security measures or that it would wait several months to notify them of a data breach involving their Private Information.

176. Defendant's breaches of contract have caused Plaintiff and Class Members to suffer damages from the lost benefit of their bargain, out of pocket monetary losses and expenses, loss of time, and diminution of the value of their Private Information.

177. As a direct and proximate result of Defendant's breaches of contract, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

COUNT III
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

178. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

179. A relationship existed between Plaintiff and Class Members and Defendant in which Plaintiff and Class Members put their trust in Defendant to protect their Private Information and Defendant accepted that trust.

180. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

181. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

182. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

183. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff and Class Members' Private Information.

184. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

185. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

186. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

187. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

188. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

189. Plaintiff and Class Members conferred a benefit on Defendant, by providing Defendant with their valuable Private Information, which was necessary for Defendant to provide banking services to Plaintiff and Class Members.

190. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information.

191. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

192. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

193. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

194. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

195. Plaintiff and Class Members have no adequate remedy at law.

196. As a direct and proximate result of Defendant's actions, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or

unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

197. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

198. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of

Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on

Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees'

compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: August 16, 2023

Respectfully Submitted,

/s/ *Gary M. Klinger*
Gary M. Klinger
Milberg Coleman Bryson Phillips Grossman, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

THE LYON FIRM
Joseph M. Lyon*
Kevin M. Cox*
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
jlyon@thelyonfirm.com

**Pro Hac Vice forthcoming*
Counsel for Plaintiff and Putative Class